Is Satoshi's dream still relevant today?

Closing remarks by Himino Ryozo, commissioner of the JFSA, at the Blockchain Global Governance Conference (BG2C) in Tokyo on August 24-25, 2020

Good evening, everyone. Thank you for your active participation over the last two days.

In October 2008, the global financial system was on the brink of a meltdown. The agents of trust and authority with decades of strong track records were all in the peril of their credibility. G7 finance ministers and central bank governors met in Washington DC in the month and the first item in their action plan was about bailing out: "Take decisive action and use all available tools to support systemically important financial institutions and prevent their failure."

In the same month, amid this crisis of confidence, Satoshi Nakamoto quietly put his Bitcoin paper on a mailing list. Satoshi described how the payment system, a core infrastructure of our economy, may be constructed fully peer-to-peer, with no trusted third party. You do not need mint bureaus, banks, regulators, central banks, finance ministries, professors, policemen, prosecutors, courts or armies to ensure that Bitcoin I received from an anonymous person is authentic and genuine. This proposition, together with the concepts used, including proof of work, time stamp, and Byzantine fault tolerance, has helped us think deep about the nature of the system we have been accustomed to.

More than a decade has passed since then. Today, we may be facing the need to think deep on the fundamental issues of trust again. The social construct of trust has several core building blocks in it, and some of them are in the process of rapid transformation.

For example, one important building block of trust is face-to-face meetings. Face-to-face meetings provide rich information on our counterparts and we

have some confidence in our animal instinct and intuition interpreting such information. But, with COVID-19, we are replacing many face-to-face meetings, from G20 meetings of ministers and governors to small evening drinks, with online communications. The model of trusting what I see directly with my eyes may require some supplements in the post-COVID era.

Another building block of trust has been reputed and well-trained professional editors, who work as gate-keepers of information. The editors of the Encyclopædia Britannica choose an eminent contributor for each entry, and we just trust and save the time to verify. But today we read entries by anonymous authors at Wikipedia first and then look at cited sources and evidences. We do not necessarily trust, but verify, as verification is generally becoming less costly.

In good old days, newspaper editors largely controlled the information disseminated in the society. Today, many look only at favorite entries in SNSs. Sometimes we simply trust what we want to trust.

The government has also been a major building block of trust. To demonstrate I am me, I present my passport or driver's license. If my business counterpart breaches the contract and betray me, I can go to the court and ask the government to enforce the obligation.

But in today's world of increased divide and geopolitical risks, people may wish to preserve alternatives to government-based trust so as not to let a single action by the government eliminate all the sources of trust on them. In addition, the effectiveness of enforcement by governments may be getting weaker due to the blurring nexus between physical locations and economic activities.

Thus, the conventional building blocks of trust may not work well as it used to be. Then how could we construct trust under the new normal? Potential alternatives and complements which come up to my mind include peer reviews, transparency, tamper-proof time-stamped records, and efficient verification processes. If they should play bigger roles, the world may indeed move in the direction Satoshi implied.

Satoshi did not eliminate trust elements from his proposed network. He replaced a trusted third party with a trusted community of nodes. We trust the community in the sense we assume that a majority of CPU power is controlled by nodes that are not cooperating to attack the network, and the assumption is based on the belief that nodes who have provided so much proof of work would not have incentive to destroy the value of Bitcoin.

The trust has thus come to depend on the enormous electricity and microchips deployed by miners. Would it not be an unacceptably wasteful use of resources? It may be, but I would argue that some sorts of "proof of work" are all around us, not just in Blockchains. Let us loosely define proof of work as a process costly enough to make others believe that only serious people with good standing can do it and that such cost would not have spent with dubious motifs. I would say that a significant part of our GDP is spent as this kind of proof of work.

Think about tons of banknotes with fine engravings on their faces, business people wearing well-tailored suits at elaborate offices in elegant buildings, repeated visits and beautifully designed presentation slides, entertainments at sophisticated restaurants, movie stars appearing on advertisement clips, neatly printed books with smart covers, a bunch of roses a Casanova hands to his lover, or marriage ceremonies at renowned cathedrals.

They have nothing to do with the intrinsic value of the banknotes, business proposals, advertised products, books, love, or marriage they are affiliated with. Trillions of tons of CO_2 are emitted, and a corresponding amount of dollars are spent, just to give the impression of trustworthiness and seriousness. Therefore, reviewing the roles of proof of work in generating trusts in our society and thinking how they could be reengineered would have a big potential to improve the efficiency and effectiveness of our social intercourse.

To address the design issues of Blockchain, we need to think deep about each of the building blocks of trust and governance, and if we succeed in thinking deeper, the resultant concepts and tools can help us expand the scope of

cooperation in the society in general.

Is Satoshi's dream still relevant today?

The process of innovation and exploration Satoshi initiated twelve years ago was indeed a radical movement, inviting us to think deep about our social construct, look at root causes, and seek fundamental instruments for change. And such endeavor should be all the more relevant in this age of Corona, fake news, hyper-globalization, and divide, which poses issues beyond superficial remedies.

Thanks again for your participation in BG2C and I look forward to continued dialogue.

Enjoy the Tokyo night. Thank you.

<center>***</center>